COMMONWEALTH OF MASSACHUSETTS
DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY

Investigation by the Department of Telecommunications and Energy on its own Motion pursuant to G.L. c. 159, §§ 12 and 16, into the collocation security policies of Verizon New England Inc. d/b/a Verizon Massachusetts	DTE 02-8

MOTION OF AT&T, SPRINT, GLOBAL NAPS, COVAD, CONVERSENT, AND ALLEGIANCE TO SUSPEND CURRENT LITIGATION PROCEEDINGS AND TO ESTABLISH AN INDUSTRY TASK FORCE ON NETWORK SECURITY IN LIEU OF DIVISIVE LITIGATION AND REQUEST FOR EXPEDITED RULING ON MOTION

Introduction

On the morning of September 11, 2001, 19 trained terrorists, organized into four teams, passed through airport security screens, hijacked four planes, and murdered over 3000 people in New York, Pennsylvania, and Virginia. In the aftermath of this attack, both the Federal and Commonwealth governments initiated programs to investigate means of strengthening the public infrastructure against terrorist attacks. The present inquiry is one such investigation.

The public telephone network of Massachusetts consists of a "network of networks" maintained by AT&T Communications of New England, Inc. ("AT&T"), Verizon Massachusetts, Inc. ("Verizon"), and other telecommunications carriers. The separate networks of these carriers must be interconnected, and the security of the points of interconnection is a matter of vital – and common – concern to all co-carriers of the Commonwealth's public telephone network.

The New York affiliates of these carriers incurred, in aggregate, hundreds of millions of dollars of losses from the attacks of September 11. They also set aside their partisan arguments

in the wake of the attack and cooperatively worked together to restore the destroyed and damaged network infrastructure.

In this proceeding, Verizon has submitted Panel Testimony that appears to misapprehend the gravity and proper focus of this proceeding. Rather than using the present forum to explore avenues by which central office and network security could be improved for the benefit of all facilities-based carriers, Verizon seeks to use this docket to re-assert anti-competitive collocation positions that this Department has previously heard and rejected.

Given the gravity of both the Department's concerns and the events that led to those concerns, it is imperative that this proceeding not be led astray. Verizon's Panel Testimony attempts to do so by advocating that carriers re-locate their collocated facilities and, in some central offices, be forced to relinquish operational control of their own facilities to Verizon via virtual collocation. Verizon's proposals do little, if anything, either to identify the legitimate security risks that terrorism and sabotage might present to Massachusetts' telecommunications networks or to propose methods for addressing those threats. Indeed, nowhere in Verizon's testimony did it even attempt to provide an assessment of the kinds of actions that would constitute potential threats to the telecommunications infrastructure of the Commonwealth. Consequently, it also has offered no demonstration that the security measures it proposes are designed to address such threats.

In fact, Verizon's Panel Testimony seems wholly unconcerned with the prospect of terrorist threats or with approaches to prevent or mitigate the effects of such attacks. Rather, its proposals appear to be singularly focused on reasserting old and long-discredited claims of risk of intra-corporate vandalism from its CLEC customers, and using those arguments to enhance Verizon's position vis-à-vis its competitors by making facilities based competition increasingly difficult and expensive.

In light of September 11, the proper concern of this proceeding must be whether the practices of Verizon and other carriers need to be modified to protect against hostile conduct designed to harm the telecommunications infrastructure of the Commonwealth and ultimately of the nation. It would be a tragic mistake not to undertake an analysis of such risks and to protect against them where necessary and proper. It would equally be a mistake to rush mindlessly into new methods and procedures without analysis of the kinds of risks to be protected against and the degree to which the new approaches will genuinely protect. To do either the former or the latter is to give the terrorists a victory. What is not merely wrong but unconscionable is what Verizon has attempted to do here: to cash in on the nation's risk by subverting this proceeding for purely cynical and anticompetitive objectives.

The security of the public telephone network against terrorism is a matter that should transcend partisan competitive jockeying. The Department would not fulfill its own objectives and responsibilities if this proceeding were not to produce a meaningful and candid analysis of (1) the physical and electronic risks to carriers' points of interconnection and (2) the ways in which the carriers can work cooperatively to minimize those risks. With these considerations in mind, the moving parties submit that the format for this proceeding, with its implications of adversarial process, is inappropriate to the tasks at hand.

The moving parties therefore respectfully request that the Department suspend the current litigation proceedings and establish an industry task force in order to address legitimate security issues at Verizon central offices where carriers' networks are interconnected. The benefit of proceeding in such fashion is that all local exchange carriers could frankly discuss their shared and respective experiences to accurately identify security shortcomings and strengths, and cooperatively develop and implement improvements. Since the security risks in the post-September 11 world are of industry-wide concern, an industry task force would be a far more

constructive approach to addressing the concerns of the Department and the Commonwealth. Indeed, the inter-carrier quibbling that will ensue from Verizon's proposal in the context of litigation seems grossly out of place and would be a disservice to the public interest. By contrast, in the context of an industry task force on security, carriers could share their best practices and insights and give the Department a more reliable examination of existing and potential alternative security procedures.

Argument

I. VERIZON'S PANEL TESTIMONY DOES NOT ADDRESS ANY OF THE SPECIFIC SECURITY THREATS THAT HAVE BECOME MORE PREVALENT IN THE WAKE OF SEPTEMBER 11, 2001.

While the scope of this proceeding includes a review of "access by personnel of other carriers to Verizon's central offices and other facilities," the primary purpose of this proceeding is to determine "which policies, if any, should be *strengthened* to safeguard telecommunications networks[.]" *Notice of Investigation and Public Hearing*, at 1 (emphasis supplied.) Contrary to the suggestion in Verizon's testimony, the Department's purpose here is not to eliminate virtually all access by personnel of facilities-based competitive local exchange carriers ("CLECs") to Verizon's central offices.

Verizon's Panel Testimony proposes the complete elimination of CLECs' access to some of Verizon's central offices and costly restrictions on CLECs' access to the remaining central offices. However, these recommendations lack the necessary predicate: nowhere does Verizon establish any connection between these proposals and identifiable threats of hostile actions or sabotage, which is the primary focus of this proceeding. In this respect, Verizon is seeking to subvert the important objective of this proceeding to advance its own competitive agenda.

The parties and the Department must first identify specific and realistic types of hostile action and sabotage that were not contemplated when the current collocation rules were put in place before they can design meaningful policies to address them.

Verizon's testimony asserts that there have been random incidents of CLEC employees touching Verizon equipment, yet those were the very types of concerns that Verizon raised and the Department heard and determined when it adopted the collocation rules now in place. Both the Department and the Federal Communications Commission (FCC) have already found that such concerns do not justify the costly and burdensome restrictions and separate entrance requirements that Verizon now proposes. Indeed, Verizon has not even shown how the exclusion of CLEC personnel from access to central offices will prevent the types of terrorist attacks that must be considered in a post-September 11 world.

For example, it is not at all clear how Verizon's proposed measures would prevent disruption from bombs dropped on, or airliners crashed into, a central office. Nor is it at all clear how Verizon's proposals to limit access would prevent an Oklahoma-style bombing caused by a truck parked outside of a Verizon central office. Further, it is not clear how Verizon's proposals to limit internal CLEC access would prevent the cutting of fiber lines that run into the building (as has occurred during labor actions taken by Verizon employees) or the execution of a "cyber attack" on the public telephone network. Indeed, Verizon has not shown why employees of its vendors, suppliers, and even cleaning staffs should be given access to central offices that it would deny to co-carriers of the public telephone network.

Verizon's testimony suggests that the only threat to its network is posed by the carriers with networks that are interconnected to Verizon's. Experience indicates, however, that Verizon faces a far greater risk of sabotage to its central office facilities at the hands of one of its own disgruntled employees than by a representative of another company. However, even

considerations of the risk of sabotage by Verizon's own employees still miss the point of this proceeding, which is to examine how the carriers which collectively have a stake in ensuring the security of collocated facilities can minimize the risks of attack to the network over which they commonly have stewardship.

II. VERIZON'S PROPOSAL CANNOT BE IMPLEMENTED UNDER CURRENT FCC RULES, AND PARTS OF ITS PROPOSAL VIOLATE THE TELECOMMUNICATIONS ACT OF 1996.

Verizon's cumbersome and costly CLEC relocation and access-restriction proposals are not a serious response to the Department's legitimate concerns after September 11, and the Department would only waste its valuable time on them, for two reasons. First, as discussed above, Verizon has not responded to the Department's legitimate concerns by identifying hostile threats and proposing solutions. Instead, Verizon lists a number of claimed annoyances arising from CLEC collocation and, without factual support as to their frequency or significance, simply proposes a blanket ban on CLEC presence in its central offices as a panacea. Second, Verizon's proposed collocation restrictions would violate the express provisions of the 1996 Telecommunications Act and the rules of the FCC that implement those provisions. It makes little sense to proceed with the litigation of a proposal that the Department does not have the authority to implement under current FCC rules.

The FCC has spoken loud and clear on the extent to which incumbent local exchange companies (ILECs) such as Verizon may restrict the placement of CLEC equipment in separate rooms in and the construction of separate entrances to central offices. Finding that "it would be unreasonable for the incumbent to require such separation measures as a general policy[,]" the FCC stated:

> An interpretation that would allow an incumbent to require separation of equipment or separate entrances in all cases, regardless of the potential effect on competition, would fail to properly balance the statute's competing interests. This is especially true since, in many instances,

> separated equipment and separate entrances are not needed to ensure that the incumbent is able to protect its own property.

Deployment of Wireline Services Offering Advanced Telecommunications Capability, Fourth Report and Order, CC Docket No. 98-147, FCC 01-204 (rel. August 8, 2001) ("*FCC Order*"), ¶¶ 99-100 (footnotes omitted).

Indeed, the FCC recognized the incentives of ILECs to implement restrictive collocation measures as anti-competitive devices designed to unreasonably increase CLECs' collocation costs when it limited the ability of ILECs to implement separate room and entrance requirements to very narrow circumstances. The FCC stated:

> While we recognize that incumbents, like other users of incumbent LEC premises, have a right to protect their equipment from harm, *incumbents also have incentives to overstate security concerns so as to limit physical collocation arrangements and discourage competition*. We therefore conclude that an incumbent LEC may require the separation of collocated equipment from its own equipment *only if* the proposed separated space is: (a) available in the same or a shorter time frame as non-separated space; (b) at a cost not materially higher than the cost of non-separated space; and (c) is comparable, from a technical and engineering standpoint, to non-separated space. We also conclude that an incumbent LEC may require such separation measures only where legitimate security concerns, or operational constraints unrelated to the incumbent's or any of its affiliates' or subsidiaries competitive concerns, warrant them. We believe this policy will help promote the efficient use of limited space and thereby advance the statutory preference for physical over virtual collocation. We also believe that this policy reasonably balances the congressional goal of promoting competition against the incumbent's right to use and manage its own property.

FCC Order, at ¶ 102 (emphasis added; footnotes omitted).

Clearly, Verizon's proposals in this proceeding to require the placement of CLEC equipment in separate rooms and CLEC use of separate entrances in all instances violate FCC requirements. While Verizon may impose separate room and entrance requirements in limited circumstances where it can affirmatively justify them, it may not do so as a general matter. The FCC stated:

> While *we reject an interpretation of section 251(c)(6) that would allow incumbent LECs to require, without exception, that competitors use segregated collocation space and separate entrances*, this does not mean an incumbent LEC may never make use of segregated collocation space and separate entrances. Separate entrance requirements will meet the "just, reasonable, and nondiscriminatory" standard only where a separate entrance already exists that provides access to the collocation space at issue, or where construction of such an entrance is technically feasible, and will neither artificially delay collocation provisioning nor materially increase the requesting carrier's costs. In addition, an incumbent LEC may construct or require the construction of a separated entrance only where legitimate security concerns, or operational constraints unrelated to the incumbent's or any of its affiliates' or subsidiaries competitive concerns, warrant them.

FCC Order, at ¶ 103 (emphasis added; footnotes omitted).

Moreover, Verizon's proposals to require the sequestration of CLEC equipment in separate rooms and CLEC use of separate entrances would fail to satisfy FCC requirements even if it did not – contrary to FCC requirements – impose a blanket separation requirement in all instances. Remarkably, although Verizon asserts that "a separate entrance already exists that provides access to the collocation space at issue, or [that] construction of such an entrance is technically feasible, and will neither artificially delay collocation provisioning nor materially increase the requesting carrier's costs" *id.* (footnote omitted), Verizon makes no attempt to demonstrate that this is the case in each central office to which the proposal would apply. Under the FCC's rules, Verizon would have to make such a demonstration because "[a]n incumbent LEC may require collocators to pay only for the least expensive, effective security option that is viable for the physical collocation space assigned." *Id.* (footnote omitted).

Indeed, Verizon's proposals so flagrantly violate FCC rules that even Verizon does not contend otherwise. It is apparent that Verizon does not believe that the Department has the authority to implement its proposal under current law. In its Panel Testimony on page 16, Verizon asks the Department to "seek appropriate changes to FCC rules, if necessary." It hardly

warrants mentioning that Verizon would not ask the Department to "seek appropriate changes to FCC rules" unless such changes are, in fact and in law, necessary.

Moreover, Verizon's proposal to eliminate CLEC access altogether in a number of central offices is so extreme that no change in FCC rules will make it lawful. The strong preference for physical, as opposed to virtual, collocation is not simply a matter of FCC regulatory policy. That preference is built into the Telecommunications Act of 1996, which requires ILECs to "provide, on rates, terms and conditions that are just, reasonable, and nondiscriminatory, for *physical* collocation of equipment . . . at the premises of the local exchange carrier[.]" 47 U.S.C. 251(C)(6) (emphasis added). The only two exceptions that the statute permits are technical reasons and space limitations. While security concerns may be taken into account in the terms and conditions under which physical collocation is provided, such concern cannot as a matter of law be a basis for denying physical collocation altogether.

In summary, even if this were properly a proceeding to investigate CLEC collocation rather than security threats posed to the public network, it would be a waste of the Department's time to go down the path that Verizon suggests. Verizon's proposals cannot be lawfully implemented.

Rather than devoting Department resources to a Verizon competitive agenda that does not address the Department's or the Commonwealth's concerns, and cannot in any event be implemented under current law, the Department should focus the parties's efforts on an effective examination of security matters. We believe the most productive and efficient approach would be for the convening of an industry-wide study leading to joint recommendations to the Department.

III. THE ESTABLISHMENT OF AN INDUSTRY TASK FORCE WOULD LEAD TO A MUCH MORE CONSTRUCTIVE EXAMINATION OF SECURITY PROCEDURES.

As noted previously, the issues in this proceeding transcend the competitive arguments that typically are heard and determined in DTE proceedings. Indeed, divisive litigation may work at cross-purposes to the overarching need of the Commonwealth to maximize the security of the public telephone network from realistic terrorist attacks.

In the aftermath of the September 11 attacks, the New York affiliates of AT&T, Verizon, MCI Worldcom, and other carriers worked cooperatively to restore the public telephone network. The Department can harness that cooperative spirit, and much more likely achieve the real objectives of this proceeding, by directing the parties to establish an industry task force on legitimate security concerns.

To this end, the Department should require each party to appoint representatives from its security operations to meet in a task force to identify potential security threats to the public telephone network and develop appropriate responses. The analysis and recommendations should be developed by individuals whose job is security. In such an environment, the incentives – as well as the very dynamics of the discussion – will be different and far more productive. Rather than each company advancing partisan proposals, individuals who share a joint security concern in the operation of the total telecommunications network can meet cooperatively to develop an appropriate security plan. Indeed, the moving parties would further recommend that such a task force also invite security experts from law enforcement and other fields to discuss perceived security threats and realistic measures to counter or minimize the risk of such threats.

Under this approach, the Department would continue to exercise an important role. It will be at the table during the discussions. More importantly, when the analysis is completed and

the recommendations are made, they will be presented to the Department for approval. Any disagreements that could not be resolved by industry representatives in the task force could be presented to the Department at that time for resolution.

The process described here is far more likely to address the Department's genuine security concerns than the inter-carrier quibbling that Verizon's filing appears intent upon precipitating. This is simply not an appropriate proceeding for litigation gamesmanship. The stakes are too high. A task force will produce better and more informed decisions regarding appropriate security measures.

Conclusion

As indicated above, Verizon's filing fails to address the serious concerns of the Department and instead would use the occasion of this proceeding to pursue a largely unrelated private agenda. The Commonwealth is entitled to a meaningful review of the security threats to the public telephone network and measures that should be taken by all carriers to minimize those threats. The public interest will be best served by a rejection of the largely pointless gamesmanship that Verizon's filing would draw the parties into in favor of an industry task force that deals with the real security issues. The moving parties respectfully urge the Department to suspend the current litigation proceeding and establish an industry task force on network security now, before any more time is wasted on proposals that cannot be implemented.

In addition, the moving parties respectfully request that the Department rule expeditiously on this motion so that the parties will not have to spend potentially unnecessary time and resources on the development of adversarial litigation positions and testimony. In this regard, the movants respectfully suggest that the non-moving parties be afforded only a short amount of time to reply to the motion, perhaps two to three working days.

Respectfully submitted,

AT&T COMMUNICATIONS OF NEW ENGLAND, INC.

Philip S. Shapiro
AT&T Communications of New England, Inc.
111 Washington Avenue, Suite 706
Albany, NY 12210-2213
(518) 463-2555

Jeffrey F. Jones
Kenneth W. Salinger
Jay E. Gruber
John Bennett
PALMER & DODGE LLP
111 Huntington Avenue
Boston, MA 02199-7613
(617) 239-0100

SPRINT COMMUNICATIONS COMPANY, L.P.

Craig D. Dingwall
401 9th Street, N.W., Suite 400
Washington, D.C. 20005
(202) 585-1936

GLOBAL NAPS, INC.

William J. Rooney
John O. Postl
89 Access Road, Suite B
Norwood, MA 02062
(617) 507-5121

CONVERSENT COMMUNICATIONS OF MASSACHUSETTS, LLC

Scott Sawyer
222 Richmond Street, Suite 301
Providence, RI 02903
(401) 490-6376

ALLEGIANCE TELECOM OF MASSACHUSETTS

Robert D. Shapiro
Christopher H. Kallaher
Rubin & Rudman, LLP
50 Rowes Wharf
Boston, MA 02110-3319
(617) 330-7000

COVAD COMMUNICATIONS COMPANY

Anthony Hansel
600 14th Street, N.W. Suite 750
Washington, D.C. 20005
(202) 220-0410

Dated: April 23, 2002